U.S. Cyber Command members work in the Integrated Cyber Center, Joint Operations Center at Fort George G. Meade, MD, April 2, 2021. (Photo by Josef Cole)

5th Generation Warfare Already at Play

By Jesse Robert

An earlier, extended version of this article was previously published on standupamericaus.org and is republished here in abbreviated form with permission.

The ongoing strategic competition between democratic nations and authoritarian regimes, particularly led by China, represents a critical shift in global dynamics. This competition encompasses economic, military, and ideological realms, with adversaries employing advanced tactics to disrupt the established international order. The emergence of fifth-generation warfare (5GW) highlights the need for innovative strategies that can effectively address these challenges. This form of warfare, characterized by its focus on cognitive and informational strategies, aims to influence perceptions and behaviors rather than engage in direct military confrontation, necessitating a reassessment of traditional defense mechanisms.

The U.S. remains in an intense strategic competition where adversaries, especially authoritarian regimes, are rapidly advancing their economic, military, and ideological capabilities. Irregular warfare (IW) is defined as a "violent struggle among state and non-state actors for legitimacy and influence over populations," using asymmetric tactics to erode an enemy's will by targeting political authority rather than solely seeking military defeat. Cognitive warfare is considered a tool within IW, targeting how people process information. It uses psychological operations, information campaigns, and narrative control to manipulate perceptions and behavior. 5GW is described as a paradigm shift emphasizing non-traditional methods in the "gray zone." It leverages advanced technology such as artificial intelligence, cyberattacks, social engineering, and social media, alongside deniable tactics to sow confusion and instability in societies. These definitions underscore that modern conflict focuses on shaping minds and societies rather than conventional battles.

Global Threats and Authoritarian Influence

China and Russia are the primary adversaries shaping the 5GW landscape. Chinese strategy is rooted in a "Middle Kingdom" ideology that seeks to reshape the international order in favor of state control over individuals. China, along with aligned globalist entities like the United Nations (UN) and World Economic Forum (WEF), is perceived as working to erode Western norms, trust, and cohesion. Russia and other powers also employ economic and cognitive warfare against the United States. Even in Western democracies, there is a drift toward

"liberal authoritarianism," with political movements in Canada and Europe influenced by culturally Marxist ideas that weaken democratic values. Mass migration and ideological subversion in allied countries represent coordinated challenges to the rules-based order.

Information and Propaganda Tactics

5GW is primarily fought in the information domain. Adversaries exploit propaganda and digital media to destabilize societies and amplify division. The author observes that social media platforms—ranging from TikTok to podcasts and television—allow rapid, targeted influence campaigns that play on subconscious biases. Foreign intelligence agencies—such as China's People's Liberation Army, Russia, and Iran—and even some Western institutions are said to conduct covert information operations aimed at polarizing the U.S. population. These campaigns mix truth and disinformation in a way that sows public confusion and mistrust of traditional institutions. This "information domain" battle is a quiet yet very pervasive constant struggle over narratives, news media, and online content that shape the "cognitive reality" of American society.

Propaganda and Influence Case Studies

Cognitive warfare, integral to irregular warfare, manipulates perceptions and behaviors to erode the legitimacy and influence of adversarial states. It employs a variety of tactics, including psychological operations and misinformation, to create discord and undermine societal cohesion. The latest U.S. military doctrines emphasize the importance of understanding and countering these tactics, which operate below the threshold of armed conflict. By utilizing advanced technologies like artificial intelligence and social media, adversaries can conduct operations that are often difficult to attribute, complicating responses and increasing the effectiveness of their strategies.

An example of propaganda in action is Hamas's Gaza Ministry of Health casualty reports in 2025, which were likely highly inflated for maximum propaganda impact (e.g. emphasizing women, and especially, children casualties). It is also noted that U.S. government-funded media—such as USAID, Voice of America, NPR, and PBS—have historically broadcast narratives for foreign audiences. However, some of this apparatus was used to influence American news consumption until recent reforms. On the diplomatic front, China's economic diplomacy in Central America should be highlighted. Honduras, after failing to secure Taiwanese aid, quickly turned to China for investment, illustrating Beijing's leverage to draw states away from Taiwan. Similar shifts have occurred in El Salvador, Nicaragua, and other countries. These cases highlight how state and non-state actors use information and economic carrots as tools of influence, shaping public perceptions and altering geopolitical alignments through seemingly benign means.

U.S. Vulnerabilities and Countermeasures

The implications of cognitive warfare and 5GW extend beyond military considerations, reaching into the realm of societal integrity and democratic values. As authoritarian regimes promote ideologies that prioritize state control over individual freedoms, the risk of societal polarization and erosion of institutional trust grows. This manipulation of public perception is particularly evident in the context of international conflicts, where misinformation and disinformation can skew narratives and influence public opinion significantly. The role of media in shaping these narratives reinforces the need for enhanced media literacy initiatives to bolster societal resilience against such divisive tactics.

There are several U.S. vulnerabilities to 5GW. Persistent social polarization and declining trust in institutions are viewed as creating openings for adversaries. Insider threats include various ideological groups— ranging from secular socialist and Marxist organizations to Islamist and antifascist activists—that are ideologically aligned against traditional American values. Bias in the news media stemming from generations of journalists educated in left-leaning universities may propagate "cultural Marxist" narratives. Financiers like Bill Gates and George Soros are often cited as shaping press perspectives and prolonging false narratives. To counter these vulnerabilities, we must have cognitive resilience, which equates to educating the public in media and information literacy and building "immunity" to disinformation. The United States must bolster a broad counterintelligence framework by reorganizing agencies to detect and neutralize domestic influence operations while reinforcing civic norms.

Counterintelligence Imperative

In my opinion, counterintelligence (CI), civil affairs, and psychological operations are all critical in defending against 5GW threats posed by adversary states and ideologies. Many experts warn that U.S. CI efforts have been inadequate against Chinese espionage efforts alone. CI must protect not only state and government secrets but also the nation's "moral Judeo-Christian and democratic-based" values. CI agencies are seen as the frontline for identifying foreign agents and influence schemes, utilizing double agents and advanced surveillance to preempt efforts that seek to manipulate American politics or degrade the country's information space. I envision an expanded CI role that includes the use of AI and data analysis to maintain ideological integrity, counter cyber-infiltration, and uphold transparent, free institutions against authoritarian subversion.

Ideological Contest: Authoritarian vs. Democratic Values

By framing 5GW as an ideological struggle, Western democratic values—such as individual freedom, transparency, and human dignity—are contrasted with authoritarian state-centric models. Authoritarian rivals,

exemplified by the Chinese Communist Party, prioritize state dominance, social control, and stability over personal liberties. If the authoritarian vision prevails globally, it could "redefine" human rights standards and marginalize democratic governance. Thus, preserving American constitutional freedoms is not only patriotic but crucial for the survival of the liberal world order. This ideological dimension means that Fourth and Fifth Generation tactics—such as propaganda, technology control, and population surveillance—are ultimately in service of a broader goal: determining whether liberal democracies or authoritarian regimes set the rules for the 21st century.

Conclusion

In conclusion, the evolving landscape of warfare necessitates a comprehensive approach to countering the multifaceted threats posed by cognitive warfare and 5GW. As democratic nations navigate this complex environment, it is imperative to prioritize the protection of societal values and institutional integrity. 5GW, cognitive/information warfare, and competing ideologies constitute a comprehensive challenge to the United States.

Understanding these subtle, non-kinetic tactics is essential to safeguarding national integrity. Defensive strategies must adapt. By fostering resilience against manipulation and misinformation, strengthening counterintelligence efforts, and reinforcing the importance of democratic principles, nations can better position themselves to confront the challenges posed by authoritarian expansionism. The stakes of this ideological struggle are high, and the preservation of democratic ideals is crucial for maintaining stability and integrity—not only for the U.S. republic but also for the global order.

Author

Jesse Robert, ATO-II, CAS, CPO, CEH, began his journey in service as a cadet with the Army JROTC and Civil Air Patrol, leading to an impressive 25-year career within the Department of Defense (DoD) defense and intelligence community. Over the years, he has served as a DoD Physical Security Specialist, Anti-Terrorism Officer, and Terrorism Liaison Officer. His dedication and performance have earned him numerous accolades, including contributing to securing two James S. Cogswell Awards for Outstanding ratings (DCSA), the Pinkerton Government Services Service Hero Award, and The Counterterrorism Group's Directors Award of Excellence. Currently pursuing his undergraduate degree in intelligence operations with a specialization in Latin America at American Military University (AMU), he is also an active member of the Society for Defense and Strategic Studies. He plans to continue his academic path by transferring to The Citadel in Charleston, South Carolina. Recently, he completed a three-year internship with The Counterterrorism Group, a subsidiary of Paladin 7 Company, where he played a key role in counterterrorism (CT) and counterintelligence (CI) operations. During this time, he served as a CT Analyst, Open Source Intelligence (OSINT) Analyst, CI Targeting Officer, and Assistant Team Lead for Open Source Intelligence Research & Development (OSINT-RDT). Mr. Robert is also deeply engaged in the study of Special Operations Forces (SOF), irregular warfare, and global conflicts. As a participant in the Irregular Warfare Center's Global Network (IWGN), he collaborates within Functional Area Networks (FANs) such as the Defense of the Homeland network, the Emerging Technology network, and the Operations in the Information Environment (OIE) network.